One of the extremely important groups is the symmetric group $S_n$. Viewing $S_n$ as symmetries of the set $\{1, \ldots, n\}$ gives us an action $S_n \curvearrowright \{1, 2, \ldots, n\}$. So, for any permutation $\sigma \in S_n$, the cyclic group $\langle \sigma \rangle \curvearrowright \{1, 2, \ldots, n\}$; and we can look at its orbits, which give us a partition of $\{1, 2, \ldots, n\}$. In a single orbit, $\sigma$ acts “cyclically,” that means if we make a directed graph with vertices $1, 2, \ldots, n$ and directed edges $(i, \sigma(i))$; then we get disjoint directed cycles.

**Ex.**

\[
\begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 \\
\sigma & & & & & \\
\end{array}
\]

\[
\begin{array}{c}
1 \\
6 \\
5 \\
\end{array}
\]

\[
\begin{array}{c}
2 \\
3 \\
\end{array}
\]

\[\{\text{mathematical symbol to code this}\}
\]

\[
(1) \ (2 \ 3 \ 5) \ (4 \ 6)
\]

\[\text{or simply}\]

\[
(2 \ 3 \ 5) \ (4 \ 6)
\]

**Def.** A permutation $\tau \in S_n$ is called a **cycle** if \( \exists c_1, \ldots, c_k \) s.t. $\tau = (c_1 \ldots c_k)$; that means $\tau(c_i) = c_{i+1}$ if $i < k$, and $\tau(c_k) = c_1$, and $\tau(x) = x$ if $x \notin \{c_1, \ldots, c_k\} \setminus \{c_1, \ldots, c_k\}$. 
Lecture 11: Support and fixed points; disjointness

Sunday, October 22, 2017 9:05 PM

Def. For \( o \in S_n \), let \( \text{Fix}(o) = \{ 1 \leq i \leq n \mid o(i) = i \} \) and \( \text{supp}(o) := \{ 1 \leq i \leq n \setminus \text{Fix}(o) \} \).

We say \( o_1, o_2 \in S_n \) are disjoint if \( \text{supp}(o_1) \cap \text{supp}(o_2) = \emptyset \).

Notice that \( \text{Fix}(o) \) is \( <o> \)-invariant; and so should be its complement; this means \( \text{supp}(o) \) is \( <o> \)-invariant.

Lemma. Suppose \( o, \tau \in S_n \) are disjoint. Then \( o \tau = \tau o \).

Proof. \( \forall i \leq 1, \ldots, n \),

Case 1. \( \tau(i) \neq i \).

Then \( i \in \text{supp}(\tau) \Rightarrow \tau(i) \in \text{supp}(\tau) \). And so \( \tau(i) \notin \text{supp}(o) \); this implies \( o(\tau(i)) = i \) and \( o(\tau(i)) = \tau(i) \). Therefore \( o(\tau(i)) = \tau(o(\tau(i))) \).

Case 2. \( o(i) \neq i \) and \( \tau(i) = i \).

(by a similar argument, we get \( o(\tau(i)) = \tau(o(i)) \).

Case 3. \( o(i) = \tau(i) = i \).

Then \( o(\tau(i)) = i = \tau(o(\tau(i))) \).

So in any case we get \( (o \tau)(i) = (\tau o')(i) \). Hence \( o \tau = \tau o \).

Lemma. Suppose \( \tau_i \in S_n \) and \( \tau_i \)'s are pairwise disjoint. Then

for any \( i, \) \( (\tau_1 \tau_2 \ldots \tau_m)\mid_{\text{supp} \tau_i} = \tau_i \mid_{\text{supp} \tau_i} \).

In particular \( \text{supp}(\tau_1 \ldots \tau_m) = \bigcup_{i=1}^{m} \text{supp}(\tau_i) \).
Lecture 11: Support of product of disjoint permutations

Monday, October 23, 2017 11:16 AM

\[ \text{Supp}(\tau_i)'s \text{ are disjoint, } \forall i \text{ we have} \]

\[ \text{Supp}(\tau_i) \subseteq \bigcup_{j \neq i} \text{Fix } \tau_j. \]

As \( \tau_i (\text{Supp}(\tau_i)) = \text{Supp } \tau_i \), for any \( x \in \text{Supp}(\tau_i) \) we have

\[ \tau_i (\tau_1 \cdots \tau_m (x)) = \tau_i (x) \in \text{Supp}(\tau_i); \text{ and so} \]

\[ (\tau_1 \tau_2 \cdots \tau_m)(x) = \tau_i (x). \]

Since \( x \in \text{Supp } \tau_i \), \( \tau_i (x) \neq x \). Therefore \( (\tau_1 \cdots \tau_m)(x) = \tau_i (x) \neq x \).

\[ \Rightarrow \bigcup \text{Supp } \tau_i \subseteq \text{Supp}(\tau_1 \cdots \tau_m). \]

If \( x \notin \bigcup \text{supp } \tau_i \), then \( x \in \bigcap \text{Fix } \tau_i \). So \( (\tau_1 \cdots \tau_m)(x) = x \); and the claim follows. \( \blacksquare \)

Corollary. Suppose \( \tau_1, \ldots, \tau_m \in S_n \) are disjoint, \( X \subseteq \{1, 2, \ldots, n\} \) and \( |X| \geq 2 \).

Then \( X \) is an orbit of \( <\tau_1 \cdots \tau_m> \) \( \iff \) \( X \) is an orbit of \( <\tau_i> \) for some \( i \).

\[ \text{Proof:} (\Rightarrow) \text{ Let } x \in X. \text{ Since } |X| \geq 2 \text{ and } X \text{ is the } <\tau_1 \cdots \tau_m>-\text{orbit which contains } x, \text{ we have } x \in \text{Supp}(\tau_1 \cdots \tau_m). \text{ By the previous lemma } \exists! i \text{ such that } x \in \text{Supp } \tau_i. \text{ Since } \tau_1 \cdots \tau_m |_{\text{supp } \tau_i} = \tau_i |_{\text{supp } \tau_i} \text{ and } x \in \text{Supp } \tau_i, \text{ we deduce that the } <\tau_1 \cdots \tau_m>-\text{orbit } X \text{ which} \]

math200a-17-f Page 3
contains $x \in \text{Supp } \tau_i$ is a subset of $X$. Therefore by the previous lemma, $(\tau_1 \cdots \tau_m)|_X = \tau_i|_X$. Hence inductively $(\tau_1 \cdots \tau_j)^j(x) = \tau_i^j(x)$ for any $j \in \mathbb{Z}^+$; this implies $X$ is the $<\tau_i>$-orbit of $x$.

$(\Rightarrow)$ Suppose $X$ is an orbit of $\tau_i$, and $x \in X$. Then, as $|X| \geq 2$, $x \in \text{Supp } \tau_i$; and so $(\tau_1 \cdots \tau_m)(x) = \tau_i(x)$; and this is true for any $x \in X$; this means $\tau_1 \cdots \tau_m|_X = \tau_i|_X$. As $X$ is $<\tau_i>$-invariant, it is also $<\tau_1 \cdots \tau_m>$-invariant. So using inductively we have $(\tau_1 \cdots \tau_m)^j(x) = \tau_i^j(x)$; this implies the $<\tau_1 \cdots \tau_m>$-orbit of $x$ is the same as $<\tau_i>$-orbit $X$ of $x$.

**Lemma.** Let $\sigma = (i_1^{a_1} i_2^{a_2} \ldots i_k^{a_k}) \in S_n$. Suppose $k \geq 1$, $X \subseteq \{1, \ldots, n\}$, and $|X| \geq 2$. Then $X$ is a $<\sigma>$-orbit if and only if

$$X = \{i_1, \ldots, i_k\}.$$

**Proof.** $(\Rightarrow)$. $x \in X \Rightarrow |<\sigma> \cdot x| = |X| \geq 2 \Rightarrow x \in \text{Supp } \sigma \Rightarrow x \in \{i_1, \ldots, i_k\}$

$$\Rightarrow x = i_t$$ for some $t \Rightarrow X = <\sigma> i_t = \{i_1, \ldots, i_k\}$.

$(\Leftarrow)$ is clear. \[\square\]
Lemma (Uniqueness) Suppose $\tau_1, \ldots, \tau_m$ are disjoint cycles and $\sigma_1, \ldots, \sigma_k$ are disjoint cycles. Suppose $|\text{supp } \tau_i| \geq 2$ and $|\text{supp } \sigma_i| \geq 2$ (they are non-trivial). Then

$$\tau_1 \ldots \tau_m = \sigma_1 \ldots \sigma_k$$

implies $m = k$ and

$$\tau_1 = \sigma_{i_1}, \ldots, \tau_m = \sigma_{i_m}$$

where $(i_1, \ldots, i_m)$ is a permutation of $1, \ldots, m$.

Proof. We proceed by induction on $m$; with an understanding that $m=0$ means the LHS is the identity element.

Base of induction. If $k = 0$, then $\text{supp } (\sigma_1 \ldots \sigma_k) = \bigcup \text{supp } \sigma_i \neq \emptyset$ by a lemma which is proved earlier.

Induction step. Since $\tau_1$ is a non-trivial cycle, $\text{supp } \tau_1$ is a $\langle \tau_1 \rangle$-orbit of size $\geq 2$. Hence by a lemma $\text{supp } \tau_1$ is a $\langle \tau_1 \ldots \tau_m \rangle$-orbit of size $\geq 2$. Therefore $\text{supp } \tau_1$ is a $\langle \sigma_1 \ldots \sigma_k \rangle$-orbit of size $\geq 2$. Thus by a lemma $\exists \ i_1 \ s.t.$ $\text{supp } \tau_1$ is a $\langle \sigma_{i_1} \rangle$-orbit of size $\geq 2$. As $\sigma_{i_1}$ is a cycle, by a lemma, $\text{supp } \tau_1 = \text{supp } \sigma_{i_1}$. We also know
Lecture 11: Uniqueness of cycle decomposition

Monday, October 23, 2017 12:24 PM

\[ \tau_1 \mid \text{supp } \tau_1 = (\tau_1 \ldots \tau_m) \mid \text{supp } \tau_1 \]
\[ = (\sigma_1 \ldots \sigma_k) \mid \text{supp } \sigma_i \]
\[ = (\sigma_1 \ldots \sigma_k) \mid \text{supp } \sigma_i \]
\[ = \sigma_{i_1} \mid \text{supp } \sigma_i \]
\[ \text{; this implies } \tau_1 = \sigma_{i_1} \]

Now the claim follows using the induction hypothesis. \[ \blacksquare \]

**Lemma (Existence)** For any \( \sigma \in S_n \setminus \{1\} \), there are disjoint cycles \( \tau_1, \ldots, \tau_m \) such that \( \sigma = \tau_1 \ldots \tau_m \).

**Proof.** Suppose \( \langle \sigma \rangle \setminus \{1\} \rangle = \exists x_1, \ldots, x_k \). And after reordering assume \( |x_1|, \ldots, |x_m| \geq 2 \) and \( |x_{m+1}| = \ldots = |x_k| = 1 \).

For \( 1 \leq i \leq m \), let \( \tau_i \in S_n \) be \( \tau_i \mid x_i = \sigma_i \mid x_i \) and \( \tau_i \mid x_i = I \mid x_i \).

**Claim 1.** \( \tau_i \) is a cycle.

**Proof.** \( \tau_i(x_i) = \sigma_i(x_i) = x_i \Rightarrow \tau_i \) is surjective \( \Rightarrow \tau_i \in S_n \).

- \( x_i = \langle \sigma_i \rangle \cdot x = \exists x, \sigma_i(x), \ldots, \sigma_i^{-1}(x) \) \( = \exists x, \tau_i(x), \ldots, \tau_i^{-1}(x) \)
  \( \text{and } x = \sigma_i^{-1}(x) \) \( \text{and } \tau_i^{-1}(x) = x \)

So \( \tau_i = (x \sigma_i(x) \ldots \sigma_i^k(x)) \). \[ \blacksquare \]
Claim 2. \( \sigma = \tau_1 \tau_2 \cdots \tau_m. \)

**Proof.** For every \( x \in \{1, \ldots, n\} \), there exists \( i_x \) such that \( x \in X_{i_x} \). If \( i_x \geq m+1 \), then \( \sigma^i(x) = x \) and \( \tau_i(x) = x \), for any \( 1 \leq i \leq m \).

And so \( \sigma^i(x) = x = (\tau_1 \cdots \tau_m)(x) \).

If \( i_x \leq m \), then \( x \in \text{supp} \tau_{i_x} \); and so

\[
(\tau_1 \cdots \tau_m)(x) = \tau_{i_x}(x) = \sigma^i(x)
\]

And the claim follows.

By Claim 1 and Claim 2, \( \tau_1 \cdots \tau_m \) is a cycle decomposition of \( \sigma \). \( \blacksquare \)

**Proposition.** Every \( \sigma \in S_n \) can be written as a product of disjoint cycles; and this decomposition is unique up to reordering its factors. This decomposition is called the cycle decomposition of \( \sigma \).